ESPECIFICACIONES TÉCNICAS

Adquisición de Equipos de Seguridad para Protección del Correo Electrónico, Aplicaciones Web y Base de Datos del Programa Juntos

Código: 1.2.2.4

I. Antecedentes

Mediante Decreto Supremo Nº 103-2011-EF se aprobó la operación de endeudamiento externo, entre la República del Perú y el Banco Internacional de Reconstrucción y Fomento (BIRF), quienes suscribieron el Convenio de Préstamo Nº 7961-PE, con la finalidad de financiar el proyecto denominado "Cierre de Brechas en productos priorizados del Programa Estratégico Articulado Nutricional", bajo la modalidad de Enfoque Sectorial Amplio de Apoyo Financiero (Swap).

El objetivo del proyecto es apoyar la gestión del Programa Articulado Nutricional (PAN) para lograr su propósito general de reducir la desnutrición crónica infantil en el país y contribuir con el objetivo específico de una primera etapa de reducirla a 9 por ciento hacia el año 2016. En un enfoque que se orienta a reforzar la oferta, incrementar la demanda y mejorar la gestión de los servicios, a través del financiamiento complementario de un subgrupo de actividades del PAN, se propone: a) promover la demanda de los servicios de nutrición mediante el fortalecimiento de la eficacia operativa del Programa Juntos y b) mejorar la cobertura y la calidad de la oferta de servicios preventivos de salud y nutrición básicos en las comunidades donde opera Juntos.

Para lograr estos objetivos el proyecto se propone operar a través de tres componentes principales: 1) Fortalecimiento y consolidación del Programa Juntos para las familias con niños menores de 36 meses, 2) mejorar la cobertura y la calidad de la provisión de los servicios preventivos de salud y nutrición en las áreas donde opera Juntos, y 3) fortalecer la capacidad del gobierno para influir en los resultados nutricionales, mediante la mejora en la capacidad de programación presupuestaria y el seguimiento de los resultados de las actividades seleccionadas en el PAN.

Bajo este contexto, en julio del 2012 se suscribió el Convenio de Apoyo Presupuestario al Programa Articulado Nutricional, entre el Ministerio de Desarrollo e Inclusión Social - MIDIS, al que se encuentra adscrito el Programa Nacional de Apoyo Directo a los Más Pobres – JUNTOS como Unidad Ejecutora, y el Ministerio de Economía y Finanzas, a través de la Dirección General de Presupuesto Público; el cual tenía como objetivo: "Coadyuvar al uso eficiente de los recursos para una adecuada provisión de los bienes y servicios públicos, y el logro de resultados contemplados en el Programa Presupuestario Articulado Nutricional, en el marco del Presupuesto por Resultados".

En la misma fecha, también se suscribió el Convenio de Implementación del Proyecto de "Cierre de Brechas en Productos Priorizados del Programa Estratégico Articulado Nutricional" entre el Programa JUNTOS y la Unidad de Coordinación de Préstamos Sectoriales del MEF, donde el Programa JUNTOS asume el compromiso de ser el responsable técnico y por ende el responsable por la correcta implementación del Préstamo en lo concerniente al Componente 1 para el logro de los objetivos del Proyecto.

El Programa Nacional de Apoyo Directo a los Más Pobres – JUNTOS, creado el 7 de abril del 2005 mediante Decreto Supremo No. 032–2005–PCM y adscrito desde el 01

de Enero del 2012 al Ministerio de Desarrollo e Inclusión Social (MIDIS), es el encargado de realizar transferencias de incentivos monetarios, en forma directa, a las familias que afrontan situaciones de pobreza o pobreza extrema, rural y urbana; en cuya composición existen gestantes, así como niños y adolescentes hasta los 19 años.

El Programa contribuye junto a otros Programas Sociales, en el reto de superar la pobreza y la desnutrición crónica infantil en el país; así como a preservar el capital humano, principalmente en las poblaciones en riesgo y exclusión social. En ese sentido, JUNTOS asume el complejo rol de entregar en forma directa a los hogares en situación de pobreza y extrema pobreza, incentivos monetarios condicionados al cumplimiento de compromisos que asumen las madres representantes de los hogares, para atender a sus menores hijos en los establecimientos de salud y centros educativos de las zonas donde viven. Esta misión implica para JUNTOS, promover y dinamizar la oferta de los servicios sociales, para facilitar la atención de la demanda que generan los hogares a los que atiende con un enfoque de restitución de los derechos fundamentales de la persona.

A fin de apoyar en la misión de JUNTOS, la Unidad de Tecnologías de Información (UTI) del Programa debe brindar un soporte creciente de infraestructura tecnológica para su gestión, seguimiento y monitoreo de avances y resultados, la misma que debe ser protegida ante los riesgos de amenazas y ataques que podría ser objeto la plataforma tecnológica del Programa, enfocado al cumplimiento de requisitos de la Norma Técnica Peruana NTP-ISO/IEC 27001 "EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información".

Actualmente el Programa Juntos cuenta con dos (02) equipos de seguridad "Fortigate 800C", uno que funciona como equipo principal y el otro de respaldo en un esquema "activo – pasivo", el equipo de seguridad se conecta a los siguientes segmentos de red:

- ✓ Internet: Navegación a Internet de los usuarios de la Sede Central y Unidades Territoriales
- ✓ DMZ Interno: Servidores Internos
- ✓ DMZ Externo: Servidores Externos (Públicos)
- Red Interna: Red de datos de la Sede Central con un aproximado de 160 usuarios.
- IP/VPN: Unidades Territoriales interconectadas por IP/VPN (con un aproximado de 1650 usuarios)

Es importante indicar que siendo el Centro de Cómputo de la Sede Central de Programa JUNTOS, el punto neurálgico de tecnologías de la información y comunicaciones (TIC) desde el cual se brinda el soporte de Base de Datos, Telecomunicaciones, Sistemas Informáticos, como parte de la prestación de los diversos servicios que brinda al Programa, y en muchos casos con alcance a nivel de las Unidades Territoriales, se hace necesario contar con una sólida infraestructura tecnológica de Seguridad Perimetral, la misma que permita al Programa prevenir violaciones a la seguridad de la información.

Como parte del proceso de mejoras del esquema de Seguridad de la Información, que viene desarrollando la Unidad de Tecnologías de Información (UTI), se requiere la adquisición e implementación de una serie de "Equipos de Protección" que deben de funcionar conjuntamente con la Solución de Seguridad Perimetral existente minimizando los riesgos de operación asociados a TI y reduciendo la brecha de seguridad informática existente como las amenazas y ataques dirigidos hacia la plataforma tecnológica del Programa, y maximizar el uso de las prestaciones que ofrecerá la infraestructura de seguridad perimetral, con la finalidad de obtener los siguientes beneficios:

- Seguridad completa frente a todas las amenazas que llegan por el correo electrónico entrante.
- Mayor privacidad y confidencialidad de las comunicaciones electrónicas mediante el cifrado del correo.
- Contar con plantillas personalizables de cumplimiento de normativas y prevención de la pérdida de datos confidenciales a través del correo electrónico.
- Implementación de controles que permitan cumplir con los requerimientos indicados por la NTP 27001.
- Protección contra ataques de Denegación de Servicio (DoS) sobre los servidores Web de la Institución para garantizar la operación de los sistemas informáticos.
- Parchado virtual de las aplicaciones Web para prevenir la explotación de vulnerabilidades y garantizar un tiempo óptimo mientras la Institución toma las acciones necesarias para aplicar las actualizaciones respectivas a fin de garantizar la operación y estabilidad de los servidores Web.
- Protección contra ataques que busquen realizar modificaciones no autorizadas ("defacement") en los servidores Web que puedan generar un perjuicio en la imagen y credibilidad de la Institución.
- Monitoreo y Control de los principales dispositivos (Equipos de Comunicaciones y de Seguridad), con el propósito de mitigar la eventual exposición de éstos ante incidentes de seguridad informática.
- Resolución oportuna y proactiva de eventos de seguridad previamente identificados.
- Información acerca de las incidencias y reportes de eventos de seguridad que ocurran en la Red de Datos de la Sede Central, con objeto de controlar y monitorear el riesgo operacional.
- Visibilidad de los incidentes de seguridad informática que ocurran en la red de datos de la Sede Central y sedes regionales a nivel nacional.

La adquisición e implementación de equipos de protección adicionales para la solución de Seguridad Perimetral existente, comprende la provisión, instalación, configuración y puesta a punto de un conjunto de dispositivos y herramientas de software, que deben funcionar de manera óptima y compatible con los equipos y sistemas existentes.

El presente servicio se realiza como parte de las actividades programadas del Proyecto SWAP "Cierre de Brechas en productos priorizados del Programa Estratégico Articulado Nutricional", Componente 1: Fortalecimiento y Consolidación del Programa JUNTOS para las familias con niños menores de 36 meses, Subcomponente 1.2 Sistema de Información Gerencial.

II. Objetivo

Adquirir una solución informática que permita mejorar los mecanismos de seguridad existentes en el Programa JUNTOS, a fin de brindar una mayor protección al correo electrónico institucional, aplicaciones Web y Base de Datos del Programa, para una comunicación más segura y oportuna.

III. Especificaciones Técnicas

Los equipos de protección a integrarse a la arquitectura de la solución de Seguridad Perimetral existente, debe estar compuesto por lo siguiente:

- Un (01) Equipo de seguridad para el correo electrónico tipo Email Security Appliance para la protección del servicio de correo electrónico para la Sede Central del Programa JUNTOS, cuya función principal estará orientada a identificar y bloquear las diferentes amenazas de seguridad para el correo electrónico de la Institución.
- Un (01) Equipo de función específica tipo Web Aplication Firewall (WAF) para protección y mitigación de ataques contra aplicaciones y servicios Web.
- Un (01) Equipo de Protección de Base de Datos, cuya función sea el monitoreo, auditoría y control de la Base de Datos.
- Un (01) Equipo de Administración Centralizada de Solución de Seguridad de Aplicaciones WEB y Base de Datos
- Un (01) sistema de monitoreo de red, que brinde análisis en tiempo real y monitoreo continuo de la red y servidores, apoyando en la identificación de problemas para mejorar la disponibilidad de los servicios.
- Un (01) sistema de administración de eventos e información de seguridad (SIEM) que brinde una visibilidad en tiempo real de toda la actividad que se produce en todos los sistemas. De forma tal que se obtenga un conocimiento de la situación precisa y en tiempo real, así como la rapidez y la capacidad de adaptación necesaria para identificar las amenazas críticas, responder de forma inteligente y supervisar continuamente el cumplimiento de normativas como la NTP 27001.
- Deberá considerar el licenciamiento y garantías de todos los componentes de la solución por un período mínimo de 01 año, según las Especificaciones Técnicas requeridas por el Programa Nacional de Apoyo Directo a los más Pobres – JUNTOS.
- Todos los equipos deben ser nuevos y no encontrarse en estado final de venta y soporte (End of Sales, End of Life o Phase out), debe adjuntar documento del fabricante.

Características Técnicas de los Componentes y/o funcionalidades requeridas:

1. Equipo De Protección de Correo - Email Security Appliance

El equipo deberá:

Funcionalidad:

- Solución completa que incluye la capacidad de poder realizar AntiSpam, Antivirus, AntiSpyware y Control de gusanos
- Debe ser capaz de proteger correo electrónico entrante (desde Internet) y correo saliente (hacia Internet)
- Capacidad incluida de conectarse en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones antispam
- Protección contra ataques de negación de servicio por Mail Bombing
- Verificaciones de DNS en reversa para proveer protección tipo Anti-Spoofing
- Posibilidad de establecer límites en la tasa de correos enviados.
- Capacidad de soportar múltiples dominios de correo electrónico
- Posibilidad de establecer políticas por destinatario/receptor de correo electrónico por dominio, para correo entrante o correo saliente

- Capacidad de establecer perfiles (políticas) granulares de detección de SPAM y virus. Es decir, poder definir configuraciones específicas de mecanismos AntiSpam/Antivirus.
- Posibilidad de funcionar como SMTP mail gateway para servidores de correo electrónico existentes.
- Ruteo de correo basado en LDAP
- Capacidad de poder hacer cuarentena de correo, y acceder esa cuarentena mediante WebMail y POP3
- Resúmenes diarios de cuarentena
- Almacenamiento basado en políticas para decidir el almacenamiento de correo electrónico para mensajes entrantes y salientes.
- Soporte a colas de correo para mensajes fallidos, retardados y no entregables
- Capacidad de poder hacer autenticación para SMTP a través de LDAP, RADIUS, POP3 o IMAP
- Mantiene una lista de reputación de remitentes locales basado en: Número de virus enviados, cantidad de spam enviado, número de receptores equivocados
- Filtraje de archivos anexos (attachments) y contenido de mensaje de correo
- Inspección profunda de cabeceras de correo.
- Filtraje estadístico Bayesiano.
- Capacidad de bloquear usando listas en tiempo real de URIs y/o URLs de SPAM
- Filtraje por palabra prohibida
- Administración de SPAM con capacidades de Aceptar, Reenviar (Relay) Rechazar (Reject) o descartar (discard)
- Rastreo por análisis de imágenes para detectar SPAM
- Soporte a listas negras (blacklist) de terceros
- Revisión tipo lista gris o negra.
- Revisión de IPs falsificadas
- Listas negras y blancas (usuarios/IPs permitidos o negados) a nivel global por equipo y personalizado por usuario
- Soporte a rastreo antivirus/antispyware de archivos comprimidos y anidados

Posibilidad de reemplazo/edición de mensajes de notificación en Antivirus/AntiSpyware
Bloqueo por tipo de archivo en antivirus/antispyware
Persistencia de base de datos de graylist
El dispositivo debe soportar los tres siguientes métodos de operación: modo transparente (bridge), en modo Gateway (relay) y modo servidor (Donde soporte cuentas locales de correo electrónico con acceso SMTP, POP3, IMAP)

- Almacenamiento local o remoto de los correos electrónicos que han pasado a través del dispositivo.
- Utiliza un Agente de Transferencia de Correo (MTA) basado en estándares optimizado para proveer altos niveles de desempeño.
- Por seguridad y eficiencia, el sistema debe ser de propósito específico basado en un sistema operativo pre-endurecido/asegurado. No se aceptan dispositivos basados en hardware genérico y/o con sistemas operativos genéricos.
- La configuración de las políticas, reglas, notificaciones u otros necesarios para su administración deben ser factibles de estar en lenguaje español.

Administración:

- Interface de configuración vía Web (HTTP, HTTPS)
- Los administradores podrán ser por dominio y deberá poder asignarse de qué equipos (por dirección IP y máscara) puede el administrador conectarse.
- Soporte a por menos aceptarse dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only)
- Soporte a SNMP versión 1 / versión 2 usando MIBS estándares y MIBS privados con Traps basadas en umbrales.
- Soporte a registro (logging) de incidentes antivirus
- Soporte a registro (logging) de actividad antispam
- Soporte a un syslog local o externo

Reportes:

- Genera reportes de actividad analizando los archivos de bitácoras (logs) y presentar la información en tablas (forma tabular) y en forma gráfica.
- Puede generar reportes configurando reportes bajo demanda o un reporte calendarizado en intervalos específicos
- Debe incluir por lo menos 100 diferentes tipos de reportes en cinco categorías distintas, para el diferente tipo de actividad registrado
- Los reportes pueden ser generados y enviados como PDF

Alta Disponibilidad:

- Soporte para Monitoreo de enlaces
- Soporte a capacidades de configuración de equipos en Activo-Pasivo
- Soporte a sincronización de datos de correo
- Soporte a paso a equipo secundario con conservación de estado (Stateful Failover)
- Detección y notificación de falla de dispositivos cuando funcione en Alta disponibilidad

Capacidad:

- Deberá soportar como mínimo el procesamiento con controles de Antispam y antivirus de 500,000 correos por hora.
- Deberá estar licenciado para mínimo 1300 casillas, o estar licenciado de forma irrestricta.
- Deberá tener un almacenamiento como mínimo de 2 TB.
- Deberá contar como mínimo con 4 interfaces 10/100/1000.

2. Equipo de Protección para Aplicaciones Web (Web Application Firewall)

El equipo deberá:

- Proveer la posibilidad de bloquear las transacciones WEB en forma preventiva, antes de que estas lleguen vía red al servidor. El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart).
- Permitir la integración en modo Reverse Proxy Explícito, y Reverse Proxy transparente.
- Contar como mínimo con 04 interfaces Ethernet 10/100/1000BaseT.
- Detectar, alertar y opcionalmente bloquear, en tiempo real, cualquier comportamiento malicioso conocido y/o desconocido.
- Contar con un modo de aprendizaje que permita definir cuáles son las acciones esperadas y aceptadas para los usuarios.

- Traer instalada, operativa y funcionando en el mismo chasis una capacidad de 1 TB para storage.
- El modo aprendizaje, deberá aprender la estructura y elementos de la aplicación y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad. Como mínimo debe aprender sobre:
  - ❖ Hosts válidos
  - ❖ URL´s
  - ❖ Parámetros
  - ❖ Tipo de contenidos de los parámetros
  - ❖ Cookies
- En modo aprendizaje, deberá aprender además del comportamiento esperado del usuario y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad. Como mínimo debe aprender sobre:
  - ❖ Longitud del valor esperado
  - ❖ Caracteres aceptados
  - ❖ Si el parámetro es de sólo lectura o editable por el usuario
- El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento del patrón de conducta.
- A fin de asegurar la calidad de los datos auditados, la solución operando en modo bridge no debe modificar las conexiones entre los clientes y el servidor, por lo que se debe asegurar que los mismos paquetes (IP origen, IP destino, puerto origen, puerto destino, número de secuencia, #ack y datos de TCP) sean idénticos en ambas puntas.
- Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas, como mínimo:
  - ❖ Terminar las solicitudes y respuestas
  - ❖ Bloquear la sesión TCP
  - ❖ Bloquear el usuario de la aplicación
  - ❖ Bloquear la dirección IP.
- Contar con un conjunto de patrones correspondientes a los ataques conocidos. Esta base de datos de patrones debe actualizarse periódicamente en forma automática y no asistida.
- Permitir la creación de reglas lógicas que permitan identificar condiciones definidas por el usuario, cómo una expresión regular o un valor determinado, en cualquier de los siguientes elementos:
  - ❖ Encabezado y cuerpo del requerimiento HTTP
  - ❖ Encabezado y cuerpo de la respuesta HTTP
- Permitir definir para las alarmas condiciones lógicas, en la cual la alarma no se dispare si no ha ocurrido por lo menos una cantidad de veces definida, en un período de tiempo definido.
- Cumplir con todas las vulnerabilidades expresadas en el OWASP.
- Soportar el volumen de tráfico y deberá tener una latencia sub-milisegundo, para no impactar el desempeño de la aplicación Web.
- Ser capaz de analizar el tráfico HTTPS sin la necesidad actuar como terminador de las sesiones SSL.
- Tener la capacidad de proteger Web Services basados en SOAP.
- Poder aprender las estructuras de los elementos SOAP y su contenido, proponiendo la configuración.
- Tener la capacidad de soportar no menos de 100 Mbps de throughput para inspección de tráfico Web, el cual debe estar disponible en la plataforma.
- Tener la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.

- El equipo de monitoreo de aplicaciones Web, deberá:
  - ❖ Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http.
  - ❖ Inspeccionar las peticiones y respuestas http.
  - ❖ Tener la habilidad de decodificar datos a su mínima expresión y validarla.
  - ❖ Validar todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.
- Tener la capacidad de realizar un parche virtual para proteger las vulnerabilidades detectadas y deberá tener integración con scanners de vulnerabilidad.
- Disponer de la funcionalidad de búsqueda de servidores Web en la red, y la capacidad para configurar automáticamente la protección para los servidores encontrados.
- Poder ser capaz de identificar el usuario de la aplicación Web. La identificación debe persistir hasta que el usuario haya abandonado la aplicación.
- Poder identificar y mantener un registro de las sesiones Web a nivel aplicativo, por medio del seguimiento de cookies o parámetros de aplicación.
- Permitir que un usuario de El equipo defina que transacciones serán logueadas.
- Implementar en forma nativa controles Anti Scrapping, permitiendo bloquear intentos reiterados sobre un mismo URL, o parte de un URL.
- Soportar la identificación del usuario aplicativo por medio de las siguientes técnicas: HTML Form, NTLM, Kerberos y Certificados digitales.
- Soportar la generación de eventos de seguridad incluyendo el usuario aplicativo, si este efectivamente se ha logueado.
- Identificar los resultados de autenticación en formularios y poder detener ataques tipo diccionario contra los formularios.

3. Equipo de Protección de Base de Datos

El equipo deberá:

- Contar con tecnología de auto-aprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un baseline de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.
- Proporcionar alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- Generar reportes y tendencias en tiempo real, así como permitir la modificación de los mismos.
- Contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.
- El equipo no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.

- Funcionar independiente a la activación de la auditoría nativa de la base de datos.
- Contar como mínimo con 04 interfaces Ethernet 10/100/1000BaseT.
- Ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- El repositorio para el registro de la actividad en el appliance, no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante.
- Ser capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- Realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:
  - ❖ Cuestiones de configuración de la base de datos tales como nivel de parches, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas.
  - ❖ Cuestiones de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.
- Poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- Tener la capacidad de soportar como mínimo 450 Mbps de throughput para inspección de tráfico SQL, el cual debe estar disponible en la plataforma.
- Tener la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
- Apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y control de cambios.
- Traer instalada, operativa y funcionando en el mismo chasis una capacidad de 500 GB para Storage
- Monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- Monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, stored procedures, entre otros.
- Hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- Proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
- Estar compuesta por un dispositivo para uso exclusivo, para funciones de monitoreo, auditoría y control de Aplicaciones de Base de Datos.
- Manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.

- Identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, ésta actividad no deberá implicar la modificación de la aplicación y/o de la base de datos.
- Posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- Proteger contra ataques SQL y no-SQL (como buffer overflow)
- Contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
- Capacidad de alertar potenciales violaciones de la información basado en comportamiento que incluyan:
  - ❖ Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  - ❖ Acceso a datos inusuales para cierta hora del día.
  - ❖ Acceso a datos desde una ubicación (física) desconocida.
  - ❖ Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- Tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP).
- Tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.

4. Equipo para la Administración Centralizada de la Solución de Protección de Aplicaciones Web (WAF) y de la Solución de Protección de Base de Datos

El equipo deberá ser:

- Una solución basada en hardware y software que permita administrar de manera centralizada desde un equipo la solución de Protección de Aplicaciones Web y la Solución de Protección de la Base de Datos.
- La solución debe incluir un servidor central de administración en el cual residen el software de administración y los archivos de log generados por los diferentes componentes de la solución.
- La solución debe traer instalada, operativa y funcionando en el mismo chasis una capacidad de 500 GB para storage.
- El equipo de administración deberá realizar Backup diario en forma automática de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los módulos administrados y transferirlos automáticamente a un servidor remoto utilizando protocolo SSH y HTTPS.
- El almacenamiento externo de logs debe realizarse en archivos cifrados y firmados digitalmente, de modo de asegurar la integridad y confidencialidad de la información.
- La solución de administración permitirá, como mínimo, lo siguiente:
  - ❖ Agregar, eliminar o modificar la configuración en un entorno gráfico
  - ❖ Modificar las reglas de los diferentes equipos
  - ❖ Efectuar la configuración de los componentes de la solución
  - ❖ Visualizar los registros de auditoría, alertas de seguridad y eventos del sistema.

- ❖ Generar reportes ajustables por el usuario sobre todos los eventos mencionados en el punto anterior.
- Toda la configuración, administración y monitoreo de la solución se efectuará a través de la "consola de gestión".
- La comunicación entre la consola y el servidor de administración debe establecerse a través de un protocolo seguro con cifrado y autenticación por medio de usuarios locales.
- La solución debe proveer acceso mediante diferentes roles de seguridad a la consola. Estos mismos roles de seguridad deben poder ser asignados a un usuario externo de Active Directory o un usuario local de la solución.
- La solución de administración permitirá la visualización en tiempo real de los logs de actividad de los equipos de la solución y las modificaciones de configuración que los administradores pudieran efectuar.
- Debe existir una vista centralizada de los logs, entendiendo como tal, unificación de los logs de la totalidad de los componentes que conforman la solución.
- La solución de administración permitirá la notificación de un determinado evento, producto de la aplicación de una política de seguridad mediante: Email, Syslog y SNMP Trap, además de su visualizacion en la consola.
- La solución deberá permitir la definición de distintas políticas de seguridad, entendiéndose como tal, al conjunto de reglas bajo el cual estará controlada una determinada aplicación.
- Se deberá permitir elegir la política de seguridad a ser implementada en una aplicación, como así también la aplicación de políticas distintas para aplicaciones distintas.
- La solución de administración permitirá la definición de filtros, sobre todos y cada uno de los campos, soportando agrupaciones, permitiendo personalizar la información a ser visualizada.

5. Sistema de Monitoreo de Red

El software deberá:

- Ser una solución basada en software, que permita el monitoreo distribuido en tiempo real de dispositivos, aplicaciones, anchos de banda, performance de ambientes virtualizados, entre otros.
- La solución deberá contar, de manera obligatoria, al menos con las siguientes interfaces de acceso y administración:
  - ❖ Interfaz Web
  - ❖ Soporte a dispositivos móviles Black Berry, Android y Windows Mobile
  - ❖ GUI para Windows
  - ❖ Iphone
  - ❖ Deberá contar con API basada en HTTP para comunicación con otras aplicaciones
- La herramienta deberá ser capaz de realizar de manera automática el descubrimiento de los dispositivos, con solo la definición de un rango de IPs. (0-255)
- La solución deberá contar con la funcionalidad de ClusterFailover, para poder de esta forma asegurar alta disponibilidad en la solución de monitoreo entre al menos 5 nodos, y estos 5 nodos no deben significar un licenciamiento adicional.

- La solución deberá contar con soporte y monitoreo a través de los siguientes protocolos:
  - ❖ SNMP
  - ❖ WMI
  - ❖ SCH
- Adicionalmente la herramienta de manera natural, sin integraciones de productos adicionales, o complementos, debe asegurar funcionalidades y monitoreo sobre:
  - ❖ Packetsniffing, deberá cumplir con la funcionalidad de analizador de Protocolos
  - ❖ NetFlowv5/v9
  - ❖ SFlow v5
  - ❖ JFlow v5
  - ❖ QoSVoip (Quality of Service)
  - ❖ IPv4 e IPv6
  - ❖ Monitoreo base de datos
  - ❖ Aplicaciones y procesos.
  - ❖ POP, SMTP, IMAP, LDAP
- La funcionalidad de análisis de protocolos, debe ser nativa de la herramienta y no con un Plug-In o AddOn, que se adicione al framework o consola de administración.
- La solución además deberá ser capaz de monitorear ambientes virtualizados y soportar las siguientes tecnologías (VMware ESX / ESXi vía WBem, Xen, Hiper V, Virtuozzo)
- La solución deberá contar con sondas remotas, es decir, con la capacidad de monitorear dispositivos que se encuentren en sitios remotos (a través de acceso WAN), no dentro de la misma LAN, sin la necesidad de que exista una VPN que los integre y donde la data se recepcione o envíe de manera encriptada vía SSL a través de Internet.
- La solución deberá ser del tipo "AgentLess", es decir sin la necesidad de instalar agentes remotos, en los equipos o dispositivos a monitorear.
- La consola de administración deberá ser basada en AJAX y debe permitir acceso remoto vía WAN o desde un celular con una consola Light basada en HTTP (mini html), además contar con una aplicación nativa para Celulares Android y Blackberry, sin que eso represente un costo adicional, ni licencias adicionales.
- Deberá contar con niveles de acceso, seguridad y definición de perfiles.
- Deberá contar con la capacidad de armar mapas topológicos de la infraestructura descubierta, y generar las relaciones entre ellos (relaciones jerárquicas).
- La solución deberá contar con su propia base de datos, sin tener la necesidad de la implementación de una base de datos de terceros.
- La herramienta deberá contar con la funcionalidad de reportes, sin integración de productos de terceros o módulos adicionales, para la generación de reportes pre definidos, o reportes personalizados de acuerdo a las necesidades del cliente.
- La solución ofertada, deberá contar con Reportes de Niveles de Servicios.
- La solución ofertada, deberá contar con la capacidad de realizar Correlación de eventos, es decir ante una caída masiva de dispositivos, identifique la falla origen, y no alerte sucesivamente por alertas relacionadas a la misma falla reportada.
- La herramienta ofertada, deberá contar con un licenciamiento ilimitado de sensores.
- La aplicación deberá basar su licenciamiento en el uso de sensores y no en el descubrimiento de dispositivos, de esta forma, se asegura

poder reutilizar los sensores en varios dispositivos o zonas de la lan a monitorear en el caso de que se requiera y de esta forma brindar flexibilidad en el monitoreo, sin necesidad de comprar licencias adicionales.

- La solución deberá contar con monitoreo sobre el tráfico VPN.
- La solución propuesta no podrá ser del tipo Open Source, Shareware ni Freeware, la misma deberá estar respaldad por la marca, y la marca deberá tener representante comercial y de soporte en el país.
- La solución deberá contar con un único agente, y con una única licencia, sin la necesidad de incorporar módulos adicionales ó AddsOn (aunque sean del mismo fabricante) para cumplir con los requerimientos. La solución deberá contar con una UNICA licencia, y con un único Nro. De Serie para el cumplimiento de los requisitos.
- La solución ofertada deberá contar con plantillas predefinidos sobre las siguientes plataformas:
    - ❖ Microsoft Exchange Server: con el objetivo de medir la experiencia del usuario en tiempos de procesamiento y envío de mails, a través de SMTP, POP, IMAP. La herramienta deberá tener la posibilidad de monitorear, analizar y medir tiempos de entregas de un mail determinado analizando toda la trama por la cual atraviesa el paquete de datos enviado.
    - ❖ Microsoft SQL
    - ❖ Oracle
    - ❖ VMWare
    - ❖ Citrix

Asimismo deberá de considerarse dos (02) Monitores LED Full HD de 42 pulgadas como mínimo con puertos HDMI, USB, VGA, RCA; para el Monitoreo de los servicios de Red, dichos monitores deberán de ser instalados en rack móvil con giro e inclinación.

6. Equipo de Administración de Eventos e Información de Seguridad

El equipo deberá ser:

- Una solución de análisis, gestión y correlación de logs y eventos de seguridad informática en tiempo real - SIEM" a ofertar debe constar de "uno" o "varios" appliance (hardware) que incluya agentes, clientes y componentes necesarios para cumplir los requerimientos técnicos y funcionales de la entidad.
  La solución SIEM debe soportar la recolección y procesamiento de hasta 1000 eventos por segundo (EPS).
- La solución de SIEM debe contar con los siguientes componentes, estos pueden estar distribuidos (varios appliance) o encontrarse centralizados:
    - ❖ Componente de gestión, administración y operación de la solución.
    - ❖ Componente de recolección de eventos y/o log's de seguridad.
    - ❖ Componente de almacenamiento de eventos y/o log's.
    - ❖ Componente de correlación de eventos y/o log's "en tiempo real".
    - ❖ Agentes y conectores para recolectar eventos de seguridad de terceros.
    - ❖ Componente de reportes.
    - ❖ Componente de auditoría (registro de las actividades de los administradores y operadores de la solución.
- El sistema operativo del o los "appliance" debe ser basado en Linux, y deberá estar previamente endurecido por el fabricante (hardening) para garantizar un adecuado desempeño de la solución.

- La solución deberá contar con un almacenamiento interno con capacidad mínima de 3TB para almacenar eventos y log's en crudo (sin compresión) por varios días, tomando en cuenta los 1000 EPS con un tamaño de log's y eventos estimados de 400 Bytes.
- La solución deberá tener la capacidad de realizar la correlación en "TIEMPO REAL" sin necesidad de consultar la base de datos para este propósito.
- La Solución deberá permitir una gestión completa de todos sus componentes, empleando una consola de administración. Incluyendo todas las configuraciones de los dispositivos, configuración de políticas, gestión de eventos, informes, análisis, afinación de la solución, y otras funciones relevantes.
- La solución deberá soportar un mecanismo de autenticación nativo además de soportar mecanismos alternativos como: Microsoft Active Directory, Autenticación de doble factor y LDAP, los mismos que podrán ser implementados durante la etapa de instalación..

7. Servicios Complementarios

i. Instalación y Configuración

Los equipos de protección a ser provistos por EL POSTOR, contempla todo el suministro de materiales, equipos, accesorios, servicios y consumibles requeridos para la correcta instalación y puesta en operación de estos equipos.
Las actividades mínimas a realizar por parte del PROVEEDOR adjudicado son las siguientes:

- Entrega del plan de trabajo; la UTI del Programa JUNTOS, realizará la evaluación y aprobación de dicho plan.
- Instalación de los equipos.
- Pruebas, ajustes y puesta en producción. Debiendo realizarse la puesta en producción en una fecha de menor impacto para la red de datos del Programa Juntos, esta actividad tendrá una duración de dos (02) días.
- Roll-back en caso de incidentes que afecten a la continuidad de los servicios.
- Al término dela implementación y puesta en producción, EL PROVEEDOR deberá entregar un informe final y una copia detallada de todas las políticas de acceso y configuraciones de los equipos de seguridad a la UT.
- Para esta implementación el Programa JUNTOS cuenta con un gabinete con una capacidad disponible de 16 RU, para la instalación de la solución.

ii. Soporte Técnico

- El servicio de soporte técnico deberá brindarse durante el periodo de la garantía y comprende todos los equipos y sistemas que conforman el equipo de Seguridad Perimetral. El soporte será ON LINE y ON SITE. Incluye consultas técnicas, resolución de averías y configuración de los equipos. El soporte técnico deberá ser brindado por EL PROVEEDOR, bajo la modalidad de 7 x 24 por el periodo del servicio.
  - ❖ "ON LINE" para requerimientos o incidentes no críticos con un tiempo de atención máximo de 15 minutos.
  - ❖ "ON SITE" con un tiempo de respuesta no mayor a una (01) hora, para incidentes graves contados a partir del momento de la notificación por parte del Programa Juntos.

- El horario de atención será de lunes a domingo de 00:00 horas a 24:00 horas. El tiempo para la solución de problemas será de dos (02) horas como máximo.
- EL POSTOR deberá contar con un Call Center (Centro de Atención de Servicios), a través del cual, se harán los requerimientos del servicio vía llamada telefónica. Procedimiento de Atención:
  - ❖ El Programa designará el personal autorizado para realizar las solicitudes del servicio a través del Call Center del POSTOR. La solicitud del servicio se hará por llamada telefónica, el proveedor proporcionará el respectivo número telefónico.
  - ❖ La atención del servicio debe ser ON LINE (por línea telefónica o acceso remoto a los equipos, el acceso remoto se hará desde la Sede Central de Programa Juntos en Lima)
  - ❖ Solicitado el servicio EL POSTOR ingresará el requerimiento en su sistema de atención de servicios, generándole un número único de boleta de atención, con lo cual hará seguimiento al servicio hasta su ejecución. El servicio será asignado a un especialista, quien efectuará los trabajos necesarios, ya sea ON LINE u ON SITE.
  - ❖ Concluido el servicio, El POSTOR, notificará al personal autorizado de Programa Juntos para validar la atención y dará por concluido el servicio solicitado, de esta manera Programa Juntos hará seguimiento del tiempo de atención de los reportes de acuerdo a los tiempos establecidos.
- EL POSTOR debe disponer de mínimo tres (03) ESPECIALISTAS técnicos o ingenieros en electrónica, sistemas, telecomunicaciones o carreras afines con capacitación o certificación vigente en las soluciones de seguridad, deberán contar con una experiencia mínima de tres (03) años en la implementación de proyectos relacionados dentro y/o fuera del País, se debe sustentar con listado de proyectos implementados mediante declaración jurada.
- Los ESPECIALISTAS, serán responsables del soporte técnico de la Solución de Seguridad Perimetral requerida por el PROGRAMA JUNTOS, el mismo que comprende la realización de las siguientes actividades: Instalación, configuración, migración, pruebas, puesta a punto, entrada en operación y soporte de los equipos y/o sistemas durante el periodo de vigencia de la garantía. El postor deberá presentar copia de Currículum Vitae debiendo adjuntar documentación mediante la cual se acredite que dicho personal cuenta con la capacitación o certificación y la experiencia solicitada.

IV. Capacitación

El POSTOR capacitará al personal de Programa Juntos considerando lo siguiente:

- Mínimo 04 personas del Programa Juntos. Tendrá una duración mínima de 20 horas., y deberá realizarse inmediatamente después de haberse realizado la instalación de la solución.
- El proveedor adjudicado deberá remitir a los 03 días de recibido la O/C el cronograma y Syllabus del curso a capacitar. La misma que deberá ser revisada y aprobada por la Unidad de Tecnologías de Información (UTI) del Programa JUNTOS.
- El curso se dictará en las instalaciones del POSTOR, se deberá proporcionar los equipos de comunicaciones necesarios, cables de conexión, extensiones eléctricas, proyector, computadoras.

- La capacitación se realizará en Lima, el POSTOR asumirá los gastos de todos los participantes, no incluye gastos por viáticos, hospedaje ni transporte.
- Se entregará a cada participante los temas desarrollados del curso en medio impreso y archivo electrónico. Debe incluir teoría básica y trabajos de laboratorio
- El curso debe ser teórico/práctico, debe incluir prácticas de administración y configuración de los equipos.
- Una semana después de concluido el curso se deberá entregar las constancias correspondientes, solo para los participantes que aprobaron el examen con nota mínima aprobatoria de 14. Deberá indicar: título del curso, fecha y horas dictadas.

V. Otras condiciones adicionales

- EL PROVEEDOR, deberá incluir en su propuesta, el suministro de todos los materiales, equipos y accesorios consumibles requeridos para la correcta instalación del equipamiento y servicio a ser provisto, manteniendo en todo momento y circunstancia el nivel de servicio y la continuidad de las operaciones.
- En el caso de que EL PROVEEDOR, requiera realizar un corte en el servicio, éste deberá ser programado y comunicado con una semana de anticipación, la misma deberá contar necesariamente con la aprobación de la Unidad de Tecnologías de Información (UTI) del Programa JUNTOS, debiendo considerar que las actividades se realicen fuera del horario de oficina.
- El tiempo del corte de servicio programado no deberá ser mayor a 08 horas.
- Todos los equipos que conforman la solución, deben poder ser configurados y monitoreados en su totalidad como parte de su implementación.
- Todos los componentes de hardware, software, materiales y accesorios a ser instalados para la provisión del servicio serán proporcionados por el proveedor. Los componentes de hardware, necesarios para el correcto funcionamiento de la solución ofertada, deberán ser nuevos y de tecnología vigente en el mercado.
- Todos los equipos propuestos deben contar con la última versión del sistema operativo liberado por el fabricante, con opción a actualización gratuita durante el período de garantía
- Compromiso del postor de suministro de insumos, materiales o repuestos originales para el funcionamiento de la Solución por un periodo no menor de tres (03) años a partir de la fecha de las Actas de Conformidad
- EL PROVEEDOR, deberá contar con carta que acredite la representación autorizada del FABRICANTE de cada uno de los componentes de la solución a ser provista dirigida al concurso.
- EL PROVEEDOR, coordinará con la Unidad de Tecnologías de Información (UTI), la realización de los trabajos necesarios para mantener operativo la Solución de Seguridad Perimetral y poder proteger y salvaguardar la continuidad de las operaciones a nivel de los sistemas informáticos institucionales dentro de un esquema de alta disponibilidad que permita al PROGRAMA JUNTOS la continuidad de sus operaciones con normalidad.
- Cualquier incumplimiento o demora en la atención incurrirá en penalidad el PROVEEDOR.
- Los equipos y demás componentes a ser ofertados por EL PROVEEDOR, como parte del servicio deberán asegurar la compatibilidad, conectividad y operatividad entre cada uno de los dispositivos y licencias de software que integran la arquitectura tecnológica requerida por PROGRAMA JUNTOS.

VI. Garantía

- La solución ofertada debe tener una garantía de un (01) año como mínimo, respaldado mediante documento emitido por los fabricantes.
- EL PROVEEDOR deberá presentar una declaración jurada de los bienes materia de la contratación, por la cual se comprometan con el PROGRAMA JUNTOS a proveer el respaldo del fabricante de los equipos y accesorios que conforman la solución propuesta durante el tiempo de garantía ofertado.
- EL PROVEEDOR se compromete a actualizar el software base en versiones y actualizaciones que ocurran durante el período de garantía, caso contrario se considerará incumplimiento y será sujeto a un procedimiento administrativo
- La recepción conforme no enerva el derecho a reclamo por defectos o vicios ocultos. Asimismo, la recepción conforme por parte de las personas designadas por EL PROGRAMA JUNTOS no libera al PROVEEDOR de sus obligaciones en materia de garantía u otras obligaciones de acuerdo al contrato.
- Si algún equipo presente dos fallas de operación en los mismos componentes durante los primeros doce (12) meses de garantía, este deberá ser reemplazado por uno igual o de mejores características técnicas.

VII. Penalidad

- Al incurrir EL PROVEEDOR en retraso injustificado en el plazo de los entregables, Programa JUNTOS aplicará al PROVEEDOR en todos los casos, una penalidad por cada día calendario de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato.
- Adicionalmente, Programa JUNTOS podrá aplicar al PROVEEDOR una penalidad de hasta el 10% del monto a facturar, cuando se produzcan incumplimientos en los tiempos solicitados en el numeral 7 literal ii.

VIII. Productos

Los productos entregables de la presente contratación se detallan en la siguiente tabla:

Producto	Descripción	Plazo
Solución de seguridad para protección del correo electrónico, aplicaciones WEB y Base de Datos	Que considera los siguientes componentes: • Equipo De Protección de Correo - Email Security Appliance • Equipo de Protección para Aplicaciones Web (Web Application Firewall) • Equipo de Protección de Base de Datos • Equipo para la Administración Centralizada de la Solución de Protección de Aplicaciones Web (WAF) y de la Solución de Protección de Base de Datos • Software de Monitoreo de Red • Equipo de Administración de Eventos e Información de Seguridad	Hasta los sesenta (60) días calendario, a partir del día siguiente de la firma del contrato.

Producto	Descripción	Plazo
Informe de Instalación y Configuración.	Informe que contenga las actividades detalladas realizadas para la instalación y configuración de la solución.	Hasta los siete (07) días calendario posteriores a la entrega de la solución.
Acta y Constancias de Capacitación	Acta de la capacitación realizada con la firma de los participantes y constancias de participación por cada participante.	Hasta los diez (10) días calendario posteriores a la entrega de la solución.

IX. Plazo

El plazo máximo para la entrega de toda la solución no deberá exceder a los 70 días calendario y se iniciará a partir del día siguiente de firmado el contrato.

X. Costo y forma de pago

El costo total debe incluir los impuestos de ley, a ser abonado en una sola armada (100%) a la entrega de los tres productos:

N° Pago	Entregables	Porcentaje
1	• Solución de Seguridad para protección del correo electrónico, aplicaciones WEB y Base de Datos • Informe de Instalación y Configuración. • Acta de la capacitación realizada con la firma de los participantes y constancias de participación por cada participante.	100%

Los pagos serán abonados previa verificación de los entregables correspondientes, y aprobación por parte de la Unidad de Tecnologías de Información del Programa Juntos, ratificado por el Responsable Técnico de JUNTOS y la conformidad de la Dirección – Unidad de Coordinación de Préstamos Sectoriales (DUCPS).

La aprobación del Programa JUNTOS estará referida al cumplimiento de los aspectos técnicos y de la ejecución de los servicios. La aprobación de la DUCPS estará referida al cumplimiento de los aspectos formales y administrativos, vinculados a la utilización de los recursos necesarios para proceder a efectuar los pagos acordados.

XI. Coordinación y supervisión

La recepción lo realizará el personal del Almacén, con el apoyo del personal de la Coordinación Soporte y Comunicaciones (CSC) de la Unidad de Tecnologías de Información (UTI).

La conformidad se emitirá después de realizarse la instalación y puesta en producción. Estará a cargo de la Unidad de Tecnologías de Información (UTI) del programa JUNTOS, previo informe técnico de la Coordinación Soporte y Comunicaciones (CSC).

XII. Lugar de entrega y supervisión

La entrega e instalación de los equipos se realizará en la Sede Central del Programa JUNTOS, ubicado en Calle Ricardo Angulo Ramírez N° 795, Córpac – San Isidro.

Lima, Febrero del 2015.